Proof Workshop

Contents

5 Week 5: More Set Theory

5.1 Equivalence Relations

In Week 3, we mentioned that there are three relations which are ubiquitous in mathematics: equivalence relations, partial orders, and functions. We discussed functions in Week 3; today, we discuss equivalence relations.

Equivalence relations axiomize relations which "behave like =," with different types of equivalence relations capturing the ways in which two objects can be "similar but not necessarily equal to" each other.

Definition 5.1. An **equivalence relation** on a set X is a relation $R \subseteq X \times X$ satisfying the following three properties:

1. (Reflexivity) For all $x \in X$, xRx.
2. (Symmetry) For all $x, y \in X$, xRy implies yRx.
3. (Transitivity) For all $x, y, z \in X$, if xRy and yRz, then xRz.

Remark 5.2. Equivalence relations are typically denoted by symbols like $\sim$ or $\cong$. In other words, if $(x, y) \in \sim$, we write $x \sim y$. The three axioms above then become:

1. $x \sim x$;
2. $x \sim y \Rightarrow y \sim x$;

3. $(x \sim y) \wedge (y \sim z) \Rightarrow x \sim z$.

Remark 5.3. An equivalence relation cannot be defined between two different sets; in other words, there is no such thing as an equivalence relation from X to Y where $X \neq Y$.

Example 5.4.

1. The usual "equals" relation is an equivalence relation on any set X. In other words, the relation $\Delta \subseteq X \times X$ defined by $(x, y) \in \Delta$ iff $x = y$ is an equvialence relation.

2. For an integer $k > 0$, define a relation $R_k \subseteq \mathbb{N} \times \mathbb{N}$ as follows: we say that $(m, n) \in R_k$ if and only if $k \mid (m - n)$, i.e. $m - n$ is divisible by k. This is the same as saying that m and n have the same remainder when divided by k. Then R_k is an equivalence relation.

3. Let T be the set of all triangles in the plane $\mathbb{R}^2$. Define a relation $R \subseteq T \times T$ by setting $(\Delta_1, \Delta_2) \in R$ if and only if Δ_1 is similar to Δ_2. Then R is an equivalence relation.

4. Let $X = \{0, 1, 2, 3\}$. Define a relation $R \subseteq X \times X$ by setting

$$R = \{(x, y) \in X \times X : x, y \in \{0, 1\} \text{ or } x, y \in \{2, 3\}\}.$$

   Then R is an equivalence relation.

5. The relation $R \subseteq \mathbb{R} \times \mathbb{R}$ defined by

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : |x - y| < 1\}$$

   is not an equivalence relation. It fails to satisfy one of the three axioms (which one?).

6. Let X be the set of all humans. The relation on X defined by $A \sim B$ iff A is an ancestor of B is not an equivalence relation, because it is not symmetric, although it is both reflexive and transitive.

7. The relation $R \subseteq \mathbb{N} \times \mathbb{N}$ defined by $R = \{(0, 0)\}$ (in other words, $x \sim y$ if and only if $x = y = 0$) is not an equivalence relation. While it is symmetric and transitive, it is not reflexive.

5.2 Equivalence Classes

One way to think about equivalence relations is that they describe a "classification" of the elements of a set into different types. For example, consider the equivalence relation on triangles given by $\triangle_1 \sim \triangle_2$ if and only if they are similar. Two triangles are similar if and only if they have the same three angles.

Another way of thinking about this is as follows: given three angles α, β, γ which add up to 180°, let's look at the set $T_{\alpha,\beta,\gamma}$ of all triangles which have these three angles. Every triangle lies in such a set, and any two triangles in this set are similar; on the other hand, for a different set of angles α', β', γ', a triangle in $T_{\alpha',\beta',\gamma'}$ is never similar to another triangle in $T_{\alpha,\beta,\gamma}$. Hence, the equivalence relation $\sim$ describes a "classification of triangles according to angles." We can make this more general as follows.

Definition 5.5. Let X be a set and $\sim$ an equivalence relation on X. For an element $x \in X$, we define the **equivalence class of x,** denoted $[x]$, to be the set

$$[x] := \{y \in X : y \sim x\}.$$

An element $y \in [x]$ is called a **representative** of the equivalence class $[x]$.

Proposition 5.6. Let X be a set and $\sim$ an equivalence relation on X. For elements $x, y \in X$, we have $[x] = [y]$ if and only if $x \sim y$. If $[x] \neq [y]$, then they are disjoint i.e. $[x] \cap [y] = \varnothing$.

Proof. Let's begin with the first statement. Assume that $[x] = [y]$. By reflexivity, $x \in [x]$. Since $[x] = [y]$, this means that $x \in [y]$. By definition, this implies $x \sim y$.

Conversely, suppose that $x \sim y$ and let $z \in [x]$. By definition, $z \sim x$. Since $x \sim y$, we have by transitivity that $z \sim y$ and hence $z \in [y]$ by definition. Thus, we have just proven that for all $x, y \in X$, $x \sim y$ implies $[x] \subseteq [y]$. Now, $x \sim y$ also implies $y \sim x$ by symmetry. Repeating the same argument as before with y interchanged with x, we conclude that $[y] \subseteq [x]$ and hence $[x] = [y]$.

For the second statement, we prove the contrapositive. Suppose that $[x] \cap [y] \neq \varnothing$, so that $z \in [x] \cap [y]$. We need to show that $[x] = [y]$. Assume that $x' \in [x]$. By definition, $x' \sim x$. By definition, $z \sim x$. By symmetry and transitivity, this implies $x' \sim z$. Since $z \sim y$ by definition, we have by transitivity that $x' \sim y$ and hence $[x] \subseteq [y]$. Interchanging the roles of x and y in the above proof gives us $[y] \subseteq [x]$ as well, so $[x] = [y]$. □

Remark 5.7. The argument we made for the second half of the first statement and for the last statement are examples of an "argument by symmetry." In the example above, the proof of the second half of the first statement "effectively" established the following: for all $x, y \in X$, $x \sim y \Rightarrow [x] \subseteq [y]$. Since $x \sim y$ is equivalent to $y \sim x$ by symmetry, this means that we have also proven that for all $x, y \in X$, $y \sim x \Rightarrow [x] \subseteq [y]$. Hence, interchanging the variables x and y tells us that for all $x, y \in X$, $x \sim y \Rightarrow [y] \subseteq [x]$.

Definition 5.8. Let X be a set with an equivalence relation $\sim$. We define the **set of equvialence classes of X under $\sim$** to be the set

$$X/\sim := \{[x] : x \in X\}.$$

Example 5.9. Let $n > 0$ be an integer, and let $\cong_n$ be the equivalence relation on $\mathbb{Z}$ defined by $x \sim y$ iff $n \mid (x - y)$ i.e. x and y have the same remainder upon division by n. Then $\mathbb{Z}/\cong_n$ is often denoted $\mathbb{Z}/n\mathbb{Z}$ and called the **integers modulo** n. Elements of $\mathbb{Z}/n\mathbb{Z}$ are sets of the form $[x]$ where x is an integer, and $[x] = [y]$ when x and y have the same remainder upon division by n. When $n = 5$, for example, $[1]$ is an element of $\mathbb{Z}/5\mathbb{Z}$ with $[1] = [6] = [11]$.

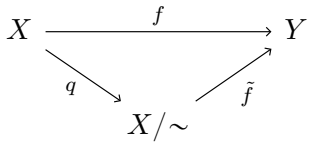
Remark 5.10. In essence, an equivalence relation defines a "partition" on a set X, which is a formalization of what it means to "split the elements of a set into different categories." In the exercises, you will have the opportunity to show that every partition defines an equivalence relation, and that every equivalence relation defines a partition via $X/\sim$.

Sometimes, we would like to be able to define a function on a set of equivalence classes. As a natural example, let's say we wanted to compute the square of the element $[3]$ in $\mathbb{Z}/5\mathbb{Z}$. I would like to be able to define $[3]^2 = [9]$. However, in $\mathbb{Z}/5\mathbb{Z}$, we have $[3] = [8]$, so another reasonable definition is $[3]^2 = [8]^2 = [64]$. In other words, in order for this function to be well-defined i.e. not give two different output for the same input, it cannot depend on the choice of representative for the particular equivalence class. An example of a "function" which is not well-defined on $\mathbb{Z}/5\mathbb{Z}$ is $f : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}$ defined by $f([x]) = x - 1$, since $f([3]) = 2 \neq 7 = f([8])$ even though $[3] = [8]$.

Proposition 5.11. Let X be a set with an equivalence relation $\sim$ and let Y be another set. Let $q : X \to X/\sim$ be the function defined by $f(x) = [x]$. If $f : X \to Y$ is a function which satisfies the property that

$$x \sim y \implies f(x) = f(y),$$

then there is a unique function $\tilde{f} : X/\sim \to Y$ such that $f = \tilde{f} \circ q$.



Proof. The condition that $f = \tilde{f} \circ q$ is equivalent to saying that for all $x \in X$, we have $f(x) = (\tilde{f} \circ q)(x) = \tilde{f}([x])$. Thus, once we show that for a function f satisfying the properties stated above, $\tilde{f}$ is well-defined, i.e. the relation $\tilde{f} \subseteq X/\sim \times Y$ given by

$$\tilde{f} = \{(S, y) \in X/\sim \times Y : \text{there is a representative } x \in S \text{ with } f(x) = y$$

is indeed a function, we are done, since this function is then unique.

Thus, we have to show that if $(S, y), (S, y') \in \tilde{f}$, then $y = y'$. Indeed, this means that there is $x \in S$ such that $f(x) = y$ and $x' \in S$ such that $f(x') = y'$. Now, since

$S \in X/\sim$, we have $S = [z]$ for some $z \in X$. Since $x \in [x] \cap [z]$, $[x] \cap [z]$ is nonempty and hence we have by Proposition 5.6 that $[x] = [z] = S$. Similarly, since $x' \in [x'] \cap [z]$, we have $[x'] = [z] = S$. Thus, $[x] = S = [x']$. By Proposition 5.6 again, this implies that $x \sim x'$. Hence, $f(x) = f(x')$ by assumption, which means that $y = f(x) = f(x') = y'$ as desired. □

Remark 5.12. You can think about the property $x \sim y \Rightarrow f(x) = f(y)$ as "f cannot distinguish $=$ from $\sim$." Thus, to specify a function on $X/\sim$ is to specify a function on X which cannot distinguish $=$ from $\sim$.

Example 5.13. Let $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the function defined by $f(x) = [x^2]$, and let $n > 0$ be an integer. If $x \cong_n y$, i.e. $n \mid (x - y)$, then $x^2 - y^2 = (x - y)(x + y)$ is also divisible by n. In other words, $x^2 \cong_n y^2$, so $[x^2] = [y^2]$. Hence, by the proposition above, the function $\tilde{f} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ which sends $\tilde{f}([x]) = [x^2]$ is well-defined.

5.3 Cardinality

We will briefly discuss cardinality and compute the cardinality of some sets. Cardinality is the measure of the size of a set according to its number of elements. Rather than trying to make sense of what it means to count the number of elements in a set on a metamathematical level, however, it is easiest to interpret cardinality as a kind of "equivalence relation on all sets."

Recall the definition of a bijection as a function $f : S \to T$ which is both injective and bijective. We proved before that this is equivalent to having an inverse $g : T \to S$. A bijection between S and T essentially gives us a one-to-one correspondence between the elements of S and the elements of T. In particular, this means that S and T have the "same number of elements."

Definition 5.14. Let S and T be two sets. We say that S and T have the same **cardinality** if there exists a bijection $f : S \to T$. In this case, we write $|S| = |T|$.

Example 5.15. The sets $\{0, 1\}$ and $\{1, 2\}$ have the same cardinality, because the map $f : \{0, 1\} \to \{1, 2\}$ sending $0 \mapsto 1$ and $1 \mapsto 2$ is a bijection. On the other hand, $\{0\}$ and $\{0, 1\}$ do not have the same cardinality, since no function $f : \{0\} \to \{0, 1\}$ is surjective.

Example 5.16. Let $p, q \in \mathbb{N}$ be two natural numbers. The sets $\{n \in \mathbb{N} : n \geqslant p\}$ and $\{n \in \mathbb{N} : n \geqslant q\}$ have the same cardinality; in particular, this means that the sets $\{0, 1, 2, \ldots\}$ has the "same number of elements" as $\{5, 6, 7, \ldots\}$, even though the latter is a strict subset of the former!

Proof. If $p = q$, then the two sets are the same, so they obviously have the same cardinality. Suppose then that $p < q$. The function

$$f : \{n \in \mathbb{N} : n \geqslant p\} \to \{n \in \mathbb{N} : n \geqslant q\}$$

sending $f(n) = n + (q - p)$ is a bijection, since it has an inverse g defined by $g(n) = n - (q - p)$. If $p > q$, we can just interchange the roles of p and q in the above proof. □

Proposition 5.17. Let X, Y, Z be sets.

1. $|X| = |X|$.
2. If $|X| = |Y|$, then $|Y| = |X|$.
3. If $|X| = |Y|$ and $|Y| = |Z|$, then $|X| = |Z|$.

Proof.

1. The function $\mathrm{id}_X : X \to X$ is a bijection, since it has an inverse, namely itself. Hence, $|X| = |X|$.
2. Suppose $|X| = |Y|$. Then there is a bijection $f : X \to Y$. Hence, f has an inverse $g : Y \to X$. g is also a bijection, since g has an inverse, namely f. Thus, $|Y| = |X|$.
3. Suppose $|X| = |Y|$ and $|Y| = |Z|$, so there exist bijections $f : X \to Y$ and $g : Y \to Z$. We claim that $g \circ f : X \to Z$ is a bijection.

   First, $g \circ f$ is injective. Suppose $x, y \in X$ such that $g(f(x)) = g(f(y))$. Since g is injective, $f(x) = f(y)$. Since f is injective, $x = y$.

   Second, $g \circ f$ is surjective. Let $z \in Z$. Since g is surjective, there exists $y \in Y$ such that $g(y) = z$. Since f is surjective, there exists $x \in X$ such that $f(x) = y$. Hence, $g(f(x)) = g(y) = z$, so $g \circ f$ is surjective. □

Remark 5.18. The proposition above *almost* says that "has equal cardinality" is an equivalence relation on all sets. We have to be careful here; as we have defined them, equivalence relations can only exist on sets, and there is no set of all sets! However, the analogy is very helpful; you can think of every set as lying in an equivalence class of sets which have the same cardinality.

5.4 Finite Sets

What does it mean for a set to have 2 elements, or 5 elements? The next definition makes this precise.

Definition 5.19. For each $n \in \mathbb{N}$, define $[n]$ to be the set

$$[n] = \{k \in \mathbb{N} : k < n\} = \{0, 1, \ldots, n - 1\}.$$

We say that a set X **has cardinality** n**,** or **has** n **elements,** if $|X| = |[n]|$. We then write $|X| = n$.

Example 5.20. The set $\varnothing$ has cardinality 0, while the set $\{0\} = [1]$ has cardinality 1. In general, each $[n]$ has cardinality n.

Example 5.21. The set $\{2, 6, 7, 3\}$ has cardinality 4, since the function $f : [4] \to \{2, 6, 7, 3\}$ sending $0 \mapsto 2$, $1 \mapsto 6$, $2 \mapsto 7$, and $3 \mapsto 3$ is a bijection.

Proposition 5.22. If X is a set with both cardinality m and cardinality n, where $m, n \in \mathbb{N}$, then $m = n$.

Proof. Do not be confused by the statement of this proposition—it is not trivial! We have defined a set X as having cardinality m if there is a bijection $[m] \to X$. But what if there were also a bijection $[n] \to X$, where $n \neq m$? Then X would have both cardinalitiy m and n! This proposition ensures that this is impossible.

We will prove the result by induction on m. If $m = 0$, then X is empty; the empty set can only have cardinality 0. Suppose now that we have proven the result for m, and X is a set with cardinality $m + 1$ and n. Then by the above argument, we must also have $n > 0$. We will use the following lemma (which we will leave as an exercise):

> If X is a set which has cardinality $n > 0$ and $x \in X$ is any element, then $X \backslash \{x\}$ has cardinality $n - 1$.

Let $x \in X$ be any element. Then $X \backslash \{x\}$ has cardinality m and $n - 1$, whence $m = n - 1$ by the induction hypothesis. Hence, $m + 1 = n$ and we are done. □

Definition 5.23. A set X is **finite** if it has cardinality n for some $n \in \mathbb{N}$. Otherwise, we say that X is **infinite.**

We will conclude with some results which may seem "obvious," but require formal proof (often by induction) to justify rigorously.

Proposition 5.24. Let X be a finite set and $S \subseteq X$. Then S is also a finite set, and $|S| \leqslant |X|$.

Proof. We will use induction on the cardinality n of X. For $n = 0$, we have $X = \varnothing$, and the only subset of $\varnothing$ is $\varnothing$, which is trivially finite and of cardinality $0 \leqslant 0$.

Now suppose the result is proven for all finite sets with cardinality n, and suppose $|X| = n + 1$. Choose any $x \in X$. If $x \notin S$, then $S \subseteq X \backslash \{x\}$. We know that $X \backslash \{x\}$ with cardinality n, so by the induction hypothesis, S is finite and $|S| \leqslant |X \backslash \{x\}| = n - 1$.

If $x \in S$, then $S \backslash \{x\} \subseteq X \backslash \{x\}$, so by the induction hypothesis, $S \backslash \{x\}$ with cardinality $k \in \mathbb{N}$. Let $f : [k] \to S \backslash \{x\}$ be a bijection.

We claim that the function $f' : [k + 1] \to S$ defined by $f'(i) = f(i)$ when $i < k$, $f'(k) = x$ is a bijection. First, we claim it is injective. Suppose that $f'(i) = f'(j)$. If $i = k$, then we must have $j = k$, since otherwise $f'(j) = f(j) \in S \backslash \{x\}$ while $f'(i) = x$, which is impossible.

If $i < k$, then we cannot have $j = k$ for the same reasoning above, so $j < k$ as well. But then $f'(i) = f(i)$ and $f'(j) = f(j)$. Since f is injective, this implies $i = j$.

Next, we claim that f' is surjective. Indeed, if $s \in S\backslash\{x\}$, then there exists $i \in [k]$ such that $f(i) = s$, and hence $f'(i) = s$. Otherwise, if $s = x$, then $f'(k) = s$. □

Remark 5.25. As a consequence of this result and the lemma above, if $S \subsetneq X$, then $|S| < |X|$ (do you see why?).

Proposition 5.26. $\mathbb{N}$ is infinite.

Proof. We will use the lemma below, that every finite subset of $\mathbb{N}$ is bounded. Suppose by contradiction that $\mathbb{N}$ is finite, so that there exists a bijection $f : [n] \to \mathbb{N}$. Then $\mathbb{N}$ is a subset of $\mathbb{N}$ which is finite, so $\mathbb{N}$ must be bounded, i.e. there exists some $b \in \mathbb{N}$ such that for all $x \in \mathbb{N}$, $b \geqslant x$. In particular, this implies $b \geqslant b + 1$, which is a contradiction. □

Lemma 5.27. Every finite subset of $\mathbb{N}$ is bounded; i.e. if $S \subseteq \mathbb{N}$ is finite, there exists a $b \in \mathbb{N}$ such that for all $x \in S$, $b \geqslant x$.

Proof. Let $S \subseteq \mathbb{N}$ be a finite subset of cardinality n. We will prove the statement by induction on n. If $n = 0$, then any $b \in \mathbb{N}$ is an upper bound for S, thus proving the base case.

Now suppose that the result is true for some $n \in \mathbb{N}$ and that $|S| = n + 1$. Let $x \in S$ be arbitrary. Then $S\backslash\{x\} \subseteq \mathbb{N}$ has cardinality n, so $S\backslash\{x\}$ has an upper bound $b \in \mathbb{N}$. If $b \geqslant x$, then b is an upper bound for S. Otherwise, if $x > b$, then x is an upper bound for S. In any case, S has an upper bound, completing the proof. □

In the exercises, you will have the opportunity to compute the cardinality of unions, cartesian products, and Hom-sets.